Docket No.: C3110.0001
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Manxia Tie et al.

Application No.: 10/534,067 Confirmation No.: 2699

Filed: January 17, 2006 Art Unit: 2431

For: A METHOD FOR THE ACCESS OF THE MOBILE TERMINAL TO THE WLAN AND FOR THE DATA COMMUNICATION VIA THE WIRELESS LINK SECURELY

Examiner: J. L. Avery

STATEMENT OF SUBSTANCE OF INTERVIEW

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

A telephone interview between Examiner Avery and applicants' undersigned representative was conducted on August 10, 2010. The following is a statement of the substance of the interview.

During the interview, applicants' undersigned representative discussed the feature of independent claim 1 that when a Mobile Terminal (MT) logs on a wireless Access Point (AP), the Mobile Terminal (MT) and the Access Point (AP) execute a two-way certificate authentication wherein a Mobile Terminal (MT) certificate and an Access Point (AP) certificate are transmitted to an Authentication Server (AS) and are authenticated through the Authentication Server (AS), then the authentication result of the Mobile Terminal (MT) certificate and the Access Point (AP) certificate is returned from the Authentication Server (AS) to the Access Point (AP) and the Mobile

Terminal (MT). The arguments and amendments made in the paper dated July 22, 2010 were also discussed.

As discussed in the interview, the authentication of certificates in Hornak is done in the issuance stage. See, e.g., paragraphs [0013] to [0014], [0018] and [0083]. For example, in Hornak, the certification authority (CA) receives a certificate-signing request (CSR) from a sender for a signed certificate. Once the sender proves its identify to the CA, the CA returns to the sender a signed certificate, that can function as, in effect, a "letter of introduction" for later communications with other parties. A receiver carries out a similar procedure with the CA to receive its own signed certificate. See, e.g., paragraphs [0013] and [0014].

However, if the sender then wants to communicate with the receiver, the sender and receiver have to perform a follow up handshake protocol, in which the sender and the receiver exchange their digital certificates *with each other*. See, id.

Thus, as was mentioned during the interview, the process set forth in Hornak is not the same as the authentication feature recited in claim 1.

The Examiner stated during the interview that in view of the most recent amendments, and the discussion, he is now inclined to agree that the claimed authentication process is different from that shown by Hornak.

The Examiner stated that he would conduct a further search of the art and issue a further action, and that in the event he does not issue a notice of allowance, the next action will be made non-final.

Dated: September 1, 2010

Respectfully submitted,

By Joseph W. Ragusa

Joseph W. Ragusa
Registration No.: 38,586
DICKSTEIN SHAPIRO LLP
1633 Broadway
New York, New York 10019-6708
(212) 277-6500
Attorney for Applicant